REMARKS

Claims 96-110 are copied substantially verbatim from U.S. Patent Application No. 09/925,072, Publication No. 2002/0023214, published February 21, 2002, for Shear et al. (hereinafter "Shear"). Added claims 96-110 correspond to Shear claims 6, 9, 10, 11, 15, 19, 21, 22, 27, 30, 31, 32, 36, 40, and 42. A one-to-one correspondence between the added claims and the Shear claims is shown in Table 1 below.

Added Claim No.	Shear Appl. Claim No.
96	6
97	9
98	10
99	11
100	15
101	19
102	21
103	22
104	27
105	30
106	31
107	32
108	36
109	40
110	42

Table 1

In accordance with 37 C.F.R. § 1.604, the copied claims may be specifically applied to Applicants' disclosure as follows:

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
96. A method of authenticating a load module comprising:	Applicants disclose a method of authenticating data packages (p.21, ll.17-31).
(a) authenticating a first digital signature associated with the load module, including the step of employing a first one-way hash algorithm, a first decryption algorithm, and a first public key; and	• Applicants disclose the use of security modules that provide sophisticated encryption, authorization algorithms, access control, and usage control. (p.10, ll.1-4). Thus, the use of a hash algorithm is at least inherently disclosed. • Applicants disclose the use of decryption modules. (p.18, ll.6-10). • Applicants disclose the use of security modules including the use of public keys. (p.21, ll.17-31). • Applicants disclose the use of extensible object security that may include multiple levels of security. (p.23, l.16-p.24, l.9).
(b) authenticating a second digital signature associated with the load module, including the step of employing at least one of:	• Applicants disclose a method of authenticating data packages (p.21, ll.17-31). • Applicants disclose the use of extensible object security that may include multiple levels of security. (p.23, l.16-p.24, l.9).
(i) a second one-way hash algorithm that is dissimilar to the first one-way hash algorithm,	• *See* Claim 96(a) above.
(ii) a second decryption algorithm that is dissimilar to the first decryption algorithm, and	Applicants disclose the use of decryption modules. (p.18, ll.6-10).

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

(iii) a second public key that is dissimilar to the first public key.	Applicants disclose the use of security modules including the use of public keys. (p.21, ll.17-31).

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
97. A protected processing environment comprising:	Applicants disclose a secure data processor (p.9, ll.8-9) including the use of passwords (p.18, ll.13-19).
means for providing a tamper resistant enclosure;	Applicants disclose the use of encryption modules, security modules, and passwords for providing a secure environment. (p.18, ll.1-5; p.18, ll.13-19).
means for maintaining at least one public verification key within the tamper resistant enclosure; and	Applicants disclose the use of security modules including the use of public keys with a secure data processor. (p.21, ll.17-31).
means for authenticating load modules based, at least in part, on use of the public verification key.	Applicants disclose the use of security modules including the use of public keys to authenticate data packages. (p.21, ll.17-31).

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
98. A method of distinguishing between trusted and untrusted load modules comprising:	Applicants disclose a method of authenticating data packages (p.21, ll.17-31).
(a) receiving a load module,	Applicants disclose a user receiving a data package. (p.19, ll.5-7; p.21, ll.24-26).
(b) determining whether the load module has an associated digital signature,	• Applicants disclose that the received data package is encrypted; in one example using RSA. (p.21, ll.18-20). • Such encryption is recognized as applying a digital signature. *See e.g.*, Shear Pub. No. US 2001/0023214 A1, para. 93 ("Two digital signature algorithms in widespread use today [include] RSA and DSA").
(c) if the load module has an associated digital signature, authenticating the digital signature using at least one secret public key; and	Applicants disclose the use of a public key to authenticate a data package. (p.21, ll.24-31).
(d) conditionally executing the load module based at least in part on the results of authenticating step (c).	Applicants disclose the use of a public key to enable usage of a data object. (p.21, ll.24-31).

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
99. A method of increasing the security of a virtual distribution environment comprising plural interoperable protected processing environments having different work factors, the method comprising:	Applicants disclose the secure transfer of two different examples of data objects, a digital image (i.e., a first load module) and a video film (i.e., a second load module), requiring different security treatment with different security modules by a user's data processor prior to usage of the data objects (i.e., the plural protected processing environments have different work factors). (p.20, l.5-p.23, l.2).
(a) classifying the plural protected processing environments based on work factor,	Applicants disclose that usage control elements define a variety of usages of the data object, for example the kind of user, allowed operations, and security modules required for use of the data object on a user's data processor (i.e., classifying the processing environments based on work factor). (p.4, ll.11-19; p.18, ll.1-5).
(b) distributing different verification public keys to different protected processing environments having different work factor classifications, and	• *See* Claim 98(c) above and Claim 99(c) below.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

(c) using the distributed verification public keys to authenticate load modules, including the step of preventing protected processing environments having different work factor classifications from executing the same load module.	• *See* Claim 98(c) and 98(d) above. • Applicants disclose that variation of object control can be applied to a particular object by creating a control data format with control elements defining the control variation and the circumstances in which the variation is applied. (p.23, ll.3-14). • Applicants further disclose that variation of object security can be applied to a particular object by creating a control data format with control elements defining the security variation and the circumstances in which the variation is applied. (p.23, ll.16-29). • Thus, it is at least inherent that control elements defining user type could include work factor classifications for the type of appliance.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
100. A protected processing environment comprising:	Applicants disclose a secure data processor (p.9, ll.8-9) including the use of passwords (p.18, ll.13-19).
a tamper resistant barrier having a first work factor; and	Applicants disclose the use of encryption modules, security modules, and passwords for providing a secure environment. (p.18, ll.1-5; p.18, ll.13-19).
at least one arrangement within the tamper resistant barrier that prevents the protected processing environment from executing the same load module accessed by a further protected processing environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.	• *See* Claim 99(c) above. • Applicants disclose the use of security modules including the use of public keys to enable usage of data objects. (p.21, ll.17-31).

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
101. A method for protecting a computation environment surrounded by a tamper resistant barrier having a first work factor, the method including:	*See* Claim 100 above.
preventing the computation environment from using the same software module accessible by a further computation environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.	• *See* Claims 99(c) and 100 above.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
102. A method of protecting computation environments comprising:	Applicants disclose a method of protecting computation environments.
(a) associating plural digital signatures with a load module;	*See* Claim 96(a) above.
(b) authenticating a first subset of the plural digital signatures with a first tamper resistant computation environment; and	• Applicants disclose that object security can include multiple levels of security utilizing methods such as encryption and keys. (p.23, ll.26-29). • *See* Claims 96(a) and 99(c) above.
(c) authenticating a second subset of the plural digital signatures with a second tamper resistant computation environment different from the first environment.	• Applicants disclose that object security can include multiple levels of security utilizing methods such as encryption and keys. (p.23, ll.26-29). • *See* Claims 96(b) and 99(c) above.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
103. A computer security method comprising:	Applicants disclose that a general set of control data comprises a security control element which defines a security procedure which has to be carried out before usage of a data object. (p.4, ll.17-19).

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

digitally signing, using a first digital signing technique, a first executable designating the first executable for use by a first device class; and	• Applicants disclose encrypting (i.e., digitally signing) control elements and a data object (i.e., a first executable) (p.4, ll.27-28; p.12, ll.15-18) to create a secure data package ready for transfer to a user (p.5, ll.7-10). Applicants disclose that usage control elements define a variety of usages of the data object, for example the kind of user, allowed operations, and security modules required for use of the data object on a user's data processor (i.e., the digital signature designates the executable for use by a device class). (p.4, ll.11-15; p.18, ll.1-5). • Applicants further disclose that the security of a data package can be improved by using a sophisticated encryption algorithm like RSA (p.21, ll.18-20) or other encryption and key methods (p.12, ll.15-18). Such usage is recognized as applying a digital signature. *See e.g.*, Shear Pub. No. US 2001/0023214 A1, para. 93 ("Two digital signature algorithms in widespread use today [include] RSA and DSA"). • Applicants disclose that the user's data processor is a general or special purpose processor (p.17, ll.2-3), data objects include books, films, video, news, music, software, games, etc. (p.2, ll.3-4), and the data object owner may want to have control over how, when, where, and by whom his property is used (p.2, ll.20-21). Applicants further disclose that object security is extensible in the sense that multiple levels of security can be applied, being dependent on the encryption/key method which is implemented in the security modules. (p.23, ll.26-29). Thus, Applicants disclose that a variety of data objects (i.e., executables) can be designated for use by data processors having certain required security modules (i.e., a device class). • Therefore, Applicants disclose digitally signing (i.e., encrypting) a first executable (i.e., a data object such as a digital image or a video file) with a first digital signature designating the first executable for use by a first device class (i.e., the encrypted control/usage elements require the user's data processor to have certain required security modules in order to use the data object).

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

digitally signing, using a second digital signing technique different from the first digital signing technique, a second executable designating the second executable for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class.	• *See* above regarding digitally signing an executable and designating a device class. • *See also* Claim 96(a) above regarding a second digital signing technique. • Applicants disclose the secure transfer of two different examples of data objects, a digital image (i.e., a first executable) and a video film (i.e., a second executable), requiring different security treatment with different security modules by a user's data processor prior to usage of the data objects (i.e., designating executables for use by devices having different tamper resistance and/or work factors). (p.20, l.5-p.23, l.2). • Applicants disclose that the general set of control data associated with a data object comprises an identifier, which uniquely identifies the general set of control data. The whole set of control data and the data object may be encrypted (i.e., digital signature of a second executable can be different from a digital signature of a first executable). (p.4, ll.19-28). • Applicants disclose that a user program comprising a usage manager module controls the usage of a data object in accordance with the control data. The user program comprises one or more security modules (i.e., user device level of security, or user device tamper resistance and/or work factor). (p.17, ll.15-20). The usage manager module applies the security modules which are necessary to use a data object. If the proper security modules are not available for a particular data object, the usage manager module will not permit usage of the data object (i.e., a second device class may have a tamper resistance and/or work factor different from the tamper resistance and/or work factor of the first device class). (p.18, ll.1-5). • Therefore, Applicants disclose digitally signing a second executable (e.g., a video file or a digital image) with a second digital signature different from the first digital signature (i.e., encrypted unique control data), the second digital signature designating the second executable for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class (i.e., encrypted control/usage elements can require the user's data processor to have different security modules in order to use different data objects).

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
104. A method of authenticating an executable comprising:	• *See* Claim 96 above. • An "executable" is equivalent to a "load module."
(a) authenticating a first digital signature associated with the executable, including the step of employing a first one-way hash algorithm, a first decryption algorithm, and a first public key; and	• *See* Claim 96(a) above. • An "executable" is equivalent to a "load module."
(b) authenticating a second digital signature associated with the executable, including the step of employing at least one of:	• *See* Claim 96(b) above. • An "executable" is equivalent to a "load module."
(i) a second one-way hash algorithm that is dissimilar to the first one-way hash algorithm,	*See* Claim 96(b)(i) above.
(ii) a second decryption algorithm that is dissimilar to the first decryption algorithm, and	*See* Claim 96(b)(ii) above.
(iii) a second public key that is dissimilar to the first public key.	*See* Claim 96(b)(iii) above.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
105. A secure execution space comprising:	*See* Claim 97 above.
means for providing a tamper resistant barrier;	• *See* Claim 97 above. • A "tamper resistant barrier" is inherent in a "tamper resistant enclosure."
means for maintaining at least one public verification key within the tamper resistant barrier; and	• *See* Claim 97 above. • A "tamper resistant barrier" is inherent in a "tamper resistant enclosure."
means for authenticating executables based, at least in part, on use of the public verification key.	*See* Claim 97 above.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
106. A method of distinguishing between trusted and untrusted executables comprising:	• *See* Claim 98 above. • An "executable" is equivalent to a "load module."
(a) receiving an executable;	• *See* Claim 98(a) above. • An "executable" is equivalent to a "load module."
(b) determining whether the executable has an associated digital signature;	• *See* Claim 98(b) above. • An "executable" is equivalent to a "load module."
(c) if the executable has an associated digital signature, authenticating the digital signature using at least one secret public key; and	• *See* Claim 98(c) above. • An "executable" is equivalent to a "load module."
(d) conditionally executing the executable based at least in part on the results of authenticating step (c).	• *See* Claim 98(d) above. • An "executable" is equivalent to a "load module."

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
107. A method of increasing the security of plural interoperable secure execution spaces having different work factors, the method comprising:	• *See* Claim 99 above. • A "secure execution space" is equivalent to a "protected processing environment."
(a) classifying the plural secure execution spaces based on work factor;	• *See* Claim 99(a) above. • A "secure execution space" is equivalent to a "protected processing environment."
(b) distributing different verification public keys to different secure execution spaces having different work factor classifications; and	• *See* Claim 99(b) above. • A "secure execution space" is equivalent to a "protected processing environment."
(c) using the distributed verification public keys to authenticate executables, including the step of preventing secure execution spaces having different work factor classifications from executing the same executable.	• *See* Claim 99(c) above. • An "executable" is equivalent to a "load module." • A "secure execution space" is equivalent to a "protected processing environment."

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
108. A protected processing environment comprising:	*See* Claim 100 above.
a tamper resistant barrier having a first work factor; and	*See* Claim 100 above.
at least one arrangement within the tamper resistant barrier that prevents the secure execution space from executing the same executable accessed by a further secure execution space having a further tamper resistant barrier with a further work factor substantially different from the first work factor.	• *See* Claim 100 above. • A "secure execution space" is equivalent to a "protected processing environment." • An "executable" is equivalent to a "load module."

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
109. A method for protecting a computation environment surrounded by	*See* Claim 101 above.
a tamper resistant barrier having a first work factor, the method including:	*See* Claim 101 above.
preventing the computation environment from using the same software module accessed by a further computation environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.	*See* Claim 101 above.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Copied Claim From InterTrust Published Patent Application (Shear et al., Pub. No. US2001/0023214 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
110. A method of protecting computation environments comprising:	*See* Claim 102 above.
(a) associating plural digital signatures with an executable;	• *See* Claim 102(a) above. • An "executable" is equivalent to a "load module."
(b) authenticating a first subset of the plural digital signatures with a first tamper resistant computation environment; and	*See* Claim 102(b) above.
(c) authenticating a second subset of the plural digital signatures with a second tamper resistant computation environment different from the first environment.	*See* Claim 102(c) above.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Pursuant to 37 C.F.R. §1.604(a)(1), Applicants propose at this time that each of the claims being copied be deemed a count for the purposes of provoking an interference. However, we reserve the right to alter the counts if necessary.

The present application was filed on May 27, 1999 as a continuation of U.S. Patent Application No. 09/164,606, filed on October 1, 1998, which in turn claimed priority to U.S. Patent Application No. 08/594,811, filed on January 31, 1996, now U.S. Patent No. 5,845,281, which in turn claimed priority to Swedish Application No. 9500355-4, filed on February 1, 1995. The present application is based on the same disclosure as U.S. Patent Application No. 08/594,811, now U.S. Patent No. 5,845,281, which contained the same disclosure as in Swedish Application No. 9500355-4. Thus, added claims 96-110 are supported by the disclosure of Swedish Application No. 9500355-4 and are entitled to a priority date of February 1, 1995.

The aforementioned added claims 96-110 are copied from U.S. Patent Application No. 09/925,072, Publication No. 2002/0023214, published on February 21, 2002 for Shear as a continuation of U.S. Patent Application No. 09/678,830, filed on October 4, 2000, now U.S. Patent No. 6,292,569, which is a continuation of U.S. Patent Application No. 08/689,754, filed on August 12, 1996, now U.S. Patent No. 6,157,721. Thus, because the present application has a priority date earlier than the priority date of Shear, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to Shear.

35 U.S.C. § 135(b)(2) does not bar this amendment because the amendment is being filed within twelve months of the publication date of the target patent application, February 21, 2002.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

CONCLUSION

Accordingly, Applicants respectfully request that an interference be declared between the present Applicants and the inventors of the aforementioned patent application. If there are any questions, please do not hesitate to call the undersigned at (949) 752-7040.

Express Mail Label No.: EV 174 798 934US

Respectfully submitted,

David S. Park
Attorney for Applicants
Reg. No. 52,094

LAW OFFICES OF
MACPHERSON KWOK
CHEN & HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049